UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/333,829	06/15/1999	TERO KIVINEN	BER-008	4596

7590 09/22/2003

RONALD C FISH
HITECH LAW
16590 OAK VIEW CIRCLE
MORGAN HILL, CA 95037

EXAMINER
SMITHERS, MATTHEWS

ART UNIT	PAPER NUMBER
2134	9

DATE MAILED: 09/22/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

3

Office Action Summary	Application No. 09/333,829	Applicant(s) KIVINEN ET AL.
	Examiner Matthew B Smithers	Art Unit 2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 July 2003* .

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-23* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Response to Arguments

Applicant's arguments filed July 25, 2003 have been fully considered but they are not persuasive.

Applicant argues Nessett does not teach a method for packets conforming to the IPsec protocol, which traditionally has not been able to traverse network address translations (NAT), to be encapsulated in another packet type (i.e. TCP or UDP) which can successfully traverse NAT. Examiner contends Nessett does teach a method in which packets conforming to the IPsec protocol can be encapsulated into another packet which can successfully traverse NATs (see column 22, line 63 to column 23, line 29). Nessett shows, in the above section, the TCP/UDP protocol data is computed after all the processing for the IPsec application has been done. Therefore, the packets conforming to the IPsec protocol are encapsulated within the TCP or UDP protocol data. Accordingly, the examiner maintains the rejection given below.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) do not apply to the examination of this application as the application being examined was not (1) filed on or after November 29, 2000, or (2) voluntarily published under 35 U.S.C. 122(b). Therefore, this application is examined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

Claims 1-23 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. patent 5,6,055,236 granted to Nessett et al.

Regarding claim 1, Nessett meets the claimed limitations as follows:

"A method for securely communicating packets between a first computer device and a second computer device through a s packet-switched data transmission network comprising intermediate computer devices, where at least one of said computer devices performs a network address translation and/or a protocol conversion, the method comprising the steps of

determining what network address translations, if any, occur on packets transmitted between the first computer device and the second computer device,

taking packets conforming to a first protocol and encapsulating them into packets conforming to a second protocol, which second protocol is capable of traversing network address translations,

transmitting said packets conforming to said second protocol from the first computer device to the second computer device and

decapsulating said transmitted packets conforming to said second protocol into packets conforming to said first protocol." see column 7, lines 8-33; column 13, line 32 to column 38, line 15 and Figure 1.

Regarding claim 2, Nessett meets the claimed limitations as follows:

"A method according to claim 1, wherein the step of taking packets conforming to a first protocol and encapsulating them into packets conforming to a second protocol comprises the substeps of taking packets conforming to the Internet Protocol, processing said packets according to the IPSEC protocol suite and encapsulating the processed packets into packets conforming to the User Datagram Protocol." see column 9, line 63 to column 10, line 4 and column 10, lines 35-40.

Regarding claim 3, Nessett meets the claimed limitations as follows:

"A method according to claim 1, wherein the step of taking packets conforming to a first protocol and encapsulating them into packets conforming to a second protocol comprises the substeps of:

taking packets conforming to the Internet Protocol,

processing said packets according to the IPSEC protocol suite and

encapsulating the processed packets into packets conforming to the Transmission Control Protocol." see column 9, lines 55-62 and column 10, lines 35-40.

Regarding claim 4, Nessett meets the claimed limitations as follows:

"A method according to claim 1, further comprising the step of compensating for the network address translations on said second protocol in the packets that are transmitted

from the first computer device to the second computer device." see column 15, line 63 to column 16, line 39.

Regarding claim 5, Nessett meets the claimed limitations as follows:

"A method according to claim 4, wherein said step of compensating for the network address translations comprises a step of performing address translation based on the information obtained in the step of determining what network address translations, if any, occur on packets transmitted between the first computer device and the second computer device." see column 15, line 63 to column 16, line 39.

Regarding claim 6, Nessett meets the claimed limitations as follows:

"A method according to claim 5, wherein said step of compensating for the network address translations further comprises a step of performing port number translation based on the information obtained in the step of determining what network address translations, if any, occur on packets transmitted between the first computer device and the second computer device." see column 15, line 63 to column 16, line 39.

Regarding claim 7, Nessett meets the claimed limitations as follows:

"A method according to claim 1, additionally comprising the step of periodically transmitting keepalive packets between the first computer device and the second computer device to ensure that the network address translations, if any, occurring on packets transmitted between the first computer device and the second computer device stay the same." see column 21, lines 17-19.

Regarding claim 8, Nessett meets the claimed limitations as follows:

"A method for conditionally setting up a secure communication connection between a first computer device and a second computer device through a packet-switched data transmission network comprising intermediate computer devices, where at least one of said computer devices performs a network address translation and/or a protocol conversion, the method comprising the steps of:

finding out, whether or not the second computer device supports a communication method where: it is determined what network address translations, if any, occur on packets transmitted between the first computer device and the second computer device; packets are taken that conform to a first protocol and encapsulated into packets that conform to a second protocol, which second protocol is capable of traversing network address translations; said packets conforming to said second protocol are transmitted from the first computer device to the second computer device; and said transmitted packets conforming to said second protocol are decapsulated into packets conforming to said first protocol,

as a response to a finding indicating that the second computer device supports said communication method, setting up a secure communication connection between the first computer device and the second computer device in which communication connection said communication method is employed and

as a response to a finding indicating that the second computer device does not support said communication method, disabling the use of said communication method between the first and the second computer devices." see column 7, lines 8-33; column 13, line 32 to column 38, line 15 and Figure 1.

Regarding claim 9, Nessett meets the claimed limitations as follows: "A method for tunnelling packets between a first computer device and a second computer device through a packet-switched data transmission network comprising intermediate computer devices, where at least one of said computer devices performs a network address translation and/or a protocol conversion, the method comprising the steps of:

establishing a bidirectional tunnelling mode between the first computer device and the second computer device by exchanging packets conforming to a secure communication protocol,

taking packets conforming to a first protocol and encapsulating them at the first computer device into packets conforming to a second protocol, which second protocol is capable of traversing network address translations,

transmitting said packets conforming to said second protocol from the first computer device to the second computer device,

decapsulating said transmitted packets conforming to said second protocol into packets conforming to said first protocol at the second computer device,

obtaining information about the address translations occurred on packets transmitted between the first computer device and the second computer device and

using said obtained information to modify the established bidirectional tunnelling mode between the first computer device and the second computer device." see column 7, lines 8-33; column 13, line 32 to column 38, line 15 and Figure 1.

Regarding claim 10, Nessett meets the claimed limitations as follows:

"A method according to claim 9, wherein the step of obtaining information about the address translations occurred on packets transmitted between the first computer device and the second computer device comprises the substeps of:

transmitting a packet between the first computer device and the second computer device, said packet comprising a header part and a payload part, and

comparing a network address transmitted in said payload part to a network address transmitted in said header part in order to find out what changes have occurred on said network address transmitted in said header part." see column 23, lines 30-45.

Regarding claim 11, Nessett meets the claimed limitations as follows:

"A method according to claim 9, additionally comprising the step of periodically transmitting keepalive packets between the first computer device and the second computer device to ensure that the network address translations, if any, occurring on packets transmitted between the first computer device and the second computer device stay the same." see column 21, lines 17-19.

Regarding claim 12, Nessett meets the claimed limitations as follows:

"A method according to claim 9, wherein the step of using said obtained information to modify the operation of the tunneling of packets comprises the substep of introducing an address translation before the encapsulation of packets in order to compensate for the network address translations that occur on packets transmitted between the first computer device and the second computer device." see column 12, line 66 to column 16, line 39.

Regarding claim 13, Nessett meets the claimed limitations as follows:

"A method according to claim 9, wherein the step of using said obtained information to modify the operation of the tunnelling of packets comprises the substep of introducing an address translation after the decapsulation of packets in order to compensate for the network address translations that occur on packets transmitted between the first computer device and the second computer device." see column 15, line 63 to column 16, line 39.

Regarding claim 14, Nessett meets the claimed limitations as follows:

"A method for tunnelling packets between a first computer device and a second computer device through a packet-switched data transmission network comprising intermediate computer devices, in which data transmission network there exists a security protocol comprising a key management connection that employs a specific packet format for key management packets, the method comprising the steps of:

encapsulating data packets that are not key management packets into said specific packet format for key management packets,

transmitting said data packets encapsulated into the specific packet format from the first computer device to the second computer device,

discriminating at the second computer device the data packets encapsulated into the specific packet format from actual key management packets and

decapsulating the data packets encapsulated into the specific packet format." see column 7, lines 8-33; column 13, line 32 to column 38, line 15 and Figure 1.

Regarding claim 15, Nessett meets the claimed limitations as follows:

"A method according to claim 14, wherein the step of encapsulating data packets that are not key management packets comprises the substeps of:

encapsulating data packets that are not key management packets into a key management packet format specified by the Internet Key Exchange protocol which defines a certain Initiator Cookie field and

inserting into the Initiator Cookie field of an encapsulated data packet a value indicating that the encapsulated packet is a data packet and not a key management packet." see column 32, line 11 to column 33, line 39.

Regarding claim 16, Nessett meets the claimed limitations as follows:
"A method for securely communicating packets between a first computer device and a second computer device through a packet-switched data transmission network comprising intermediate computer devices, where at least one of said computer devices performs a network address translation and/or a protocol conversion and where a security protocol exists comprising a key management connection, the method comprising the steps of:

for determining what network address translations, if any, occur on packets transmitted between the first computer device and the second computer device: establishing a key management connection according to said security protocol between the first computer device and the second computer device; composing an indicator packet with a header part and a payload part of which both comprise the network addresses of the first computer device and the second computer device as seen by the node composing said packet; transmitting and receiving said indicator packet within the

key management connection; and comparing in the received indicator packet the addresses contained in the header part and the payload part, and

using the information concerning the determined occurrences of network address translations to securely communicating packets between the first computer device and the second computer device." see column 7, lines 8-33; column 13, line 32 to column 38, line 15 and Figure 1.

Regarding claim 17, Nessett meets the claimed limitations as follows:

"A method according to claim 16, wherein the security protocol determines a standard port number for a key management connection, and the method further comprises the step of comparing in the received indicator packet a source port number against said standard port number for a key management connection." see column 15, lines 42-47; column 29, lines 23-33; column 30, lines 9-33; and column 36, line 62 to column 38, line 15.

Regarding claim 18, Nessett meets the claimed limitations as follows:

"A method for securely communicating packets between a first computer device and a second computer device through a packet-switched data transmission network comprising intermediate computer devices, where at least one of said computer devices performs a network address translation and/or a protocol conversion; where a security protocol is acknowledged which determines transport-mode processing of packets for transmission and reception; and where a high-level protocol checksum has been determined for checking the integrity of received packets, the method comprising the steps of:

at the first computer device, performing transport-mode processing for packets to be transmitted to the second computer device,

at the second computer device, performing transport-mode processing for packets received from the first computer device, said transport-mode processing comprising the decapsulation of received packets and

at the second computer device, updating the high-level protocol checksum for decapsulated packets for compensating for changes, if any, caused by network address translations." see column 7, lines 8-33; column 13, line 32 to column 38, line 15 and Figure 1.

Regarding claim 19, Nessett meets the claimed limitations as follows:

"A method according to claim 18, wherein

the step of performing transport-mode processing at the first computer device for packets transmitted to the second computer device takes the form of performing transport-mode processing as determined in the IPSEC protocol suite, and

the step of performing transport-mode processing at the second computer device for packets received from the first computer device takes the form of performing transport-mode processing as determined in the IPSEC protocol suite." see column 21, line 1 to column 26, line 35.

Regarding claim 20, Nessett meets the claimed limitations as follows:

"A method according to claim 18, additionally comprising the steps of:

at the first computer device, after performing transport-mode processing for a packet to be transmitted to the second computer device, encapsulating the processed packet into a packet conforming to a certain second protocol, which second protocol is capable of traversing network address translations and

at the second computer device, before performing transport-mode processing for a packet received from the first computer device, decapsulating the received packet from the packet conforming to said second protocol and replacing a number of network addresses in the decapsulated packet with a corresponding number of network addresses taken from the received packet before decapsulation." see column 21, line 1 to column 26, line 35.

Regarding claim 21, Nessett meets the claimed limitations as follows:
"A method according to claim 18, wherein the step of updating the high-level protocol checksum takes the form of recomputing the checksum for the transport-mode-processed packets." see column 23, lines 3-45.

Regarding claim 22, Nessett meets the claimed limitations as follows:
"A method according to claim 18, wherein the method additionally comprises the step of obtaining information about the network addresses of the first and second computer devices before and after network address translations, and the step of updating the high-level protocol checksum takes the form of incrementally updating the checksum based on the obtained information about the network addresses of the first and second computer devices before and after network address translations. " see column 21, line 1 to column 26, line 35.

Regarding claim 23, Nessett meets the claimed limitations as follows: "A method for maintaining the unchanged form of address translations performed by network address translation devices on encapsulated actual data packets transmitted with certain address information between a first computer device and a second computer device through a packet-switched data transmission network, the method comprising the step of:

forcing at least one of the first computer device and the second computer device to transmit to the other computer device keepalive packets with address information identical to that of actual data packets at a high enough frequency so that network

address translation devices constantly reuse the mappings used for network address translation even when a certain fraction of the packets communicated between the first computer device and the second computer device are lost in the network." see column 7, lines 8-33; column 13, line 32 to column 38, line 15 and Figure 1.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew B Smithers whose telephone number is (703) 308-9293. The examiner can normally be reached on Monday-Friday (9:00-5:30) EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A Morse can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

Matthew B Smithers
Primary Examiner
Art Unit 2134